Romain Jacquet **BTS SIO 1**
09/10/2025

Compte rendu TP05 B3: Cybersécurité - données hachées

Sommaire

Introduction 1
- **Partie 1** 2
  - **Étape 1** 2
  - **Étape 2** 2
  - **Étape 3** 3
  - **Étape 4** 4
  - **Étape 5** 4
- **Partie 2** 6

Conclusion 7

Introduction

Dans ce TP de cybersécurité, j'ai découvert le principe du **hachage de données** et son rôle dans la protection des fichiers. L'objectif était de comprendre comment une fonction de hachage permet de vérifier si un fichier a été modifié, même très légèrement. Pour cela, j'ai utilisé le logiciel **HashCalc** afin de calculer la valeur de hachage (MD5) d'un fichier texte, puis j'ai observé comment cette valeur changeait après une simple modification du contenu.

Partie 1

Étape 1

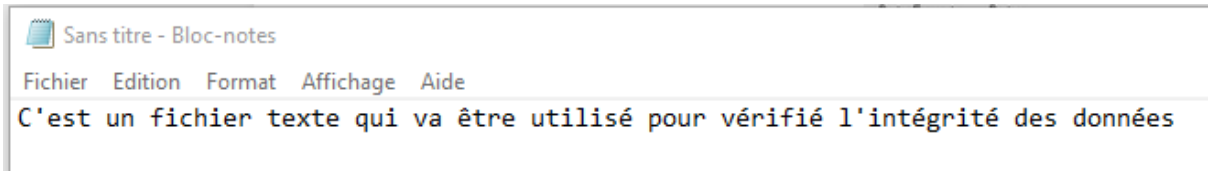
J’ai ouvert le Bloc-notes l’mon ordinateur.

J’ai tapé un texte directement dans le programme.

J’ai sélectionné **Fichier**, puis **Enregistrer**.

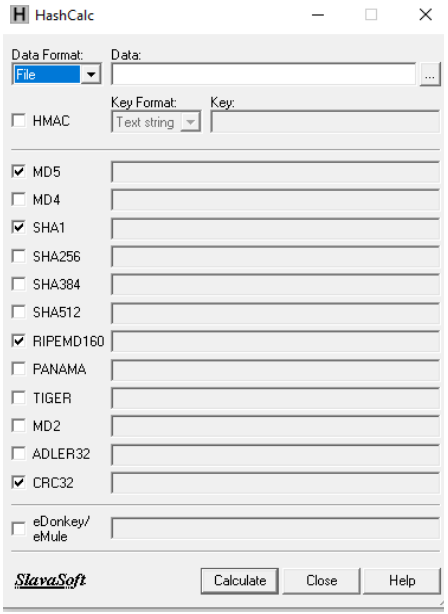
J’ai choisi d’enregistrer le fichier sur le Bureau.

J’ai entré le nom **Hash** dans le champ **Nom de fichier :** et j’ai cliqué sur **Enregistrer** pour sauvegarder le fichier.



Étape 2

J'ai ouvert un navigateur et accédé au site indiqué pour télécharger HashCalc. J'ai lancé le fichier d'installation puis suivi les instructions de l'assistant. Une fois l'installation terminée, j'ai cliqué sur "Finish" et fermé le fichier README. HashCalc est maintenant installé et prêt à être utilisé.



Étape 3

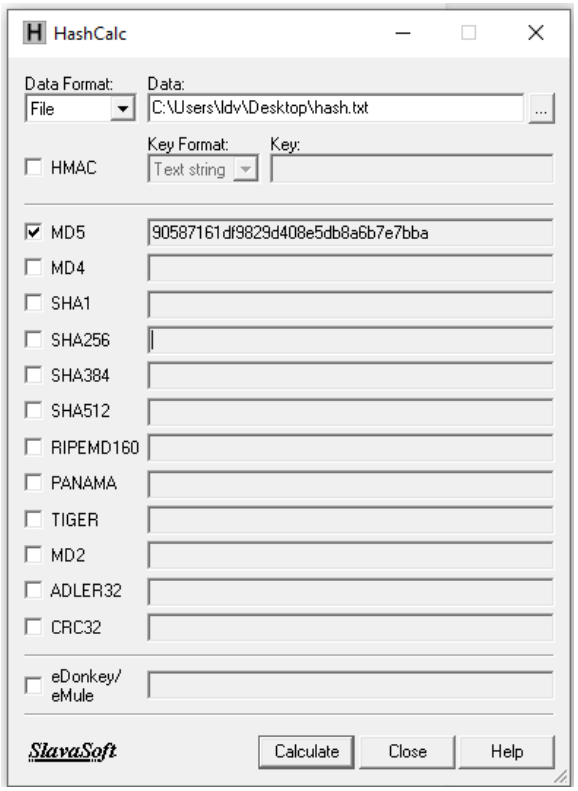
J’ai ouvert HashCalc et choisi le format File (Fichier).

J’ai cliqué sur « … » à côté de « Data » pour sélectionner le fichier Hash.txt sur le Bureau.

J’ai décoché HMAC et toutes les cases sauf MD5.

J’ai cliqué sur Calculate.

La valeur MD5 du fichier s’est affichée à côté de MD5.
90587161df9829d408e5db8a6b7e7bba

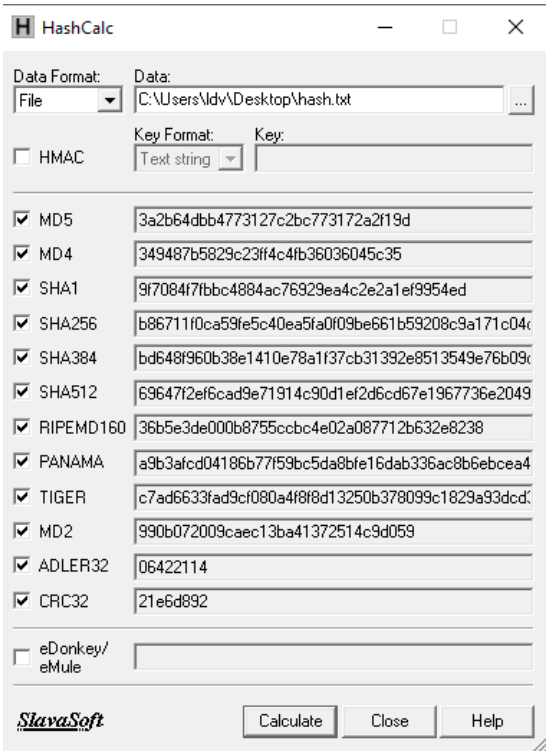


Étape 4

J’ai ouvert le fichier hash.txt sur le bureau et j’ai modifier le texte, j’ai rajouté un espace et une majuscule et j’ai sauvegardé et fermer le fichier.

Étape 5

J’ai recalculer après les modifications et la valeur qui apparaît est :
3a2b64dbb4773127c2bc773172a2f19d
La valeur et donc bien différente de celle de l’étape 3.



Partie 2

Date de l'incident	Entreprise touché	Nombres de victimes données volées	Méthodes utilisées Mesure(s) de protection prise(s)	Source de référent
Juillet 2025	Qantas	~5+ millions de clients affectés	Accès via un fournisseur tiers / compromission de base de données ; social engineering rapporté. Enquête avec experts externes, injonction judiciaire pour limiter diffusion, renforcement des sécurités côté fournisseur et recommandations aux clients (surveillance, vigilance phishing).	https://www.reuters.com/sustainability/boards-policy-regulation/qantas-says-customer-data-released-by-cyber-criminals-months-after-cyber-breach-2025-10-12/
20 décembre 2023	First american financial	centaines de million	Accès non autorisé aux systèmes (exfiltration + chiffrement dans certains cas) — exploitation de systèmes non-productifs et vulnérabilités internes. Notifications, analyse forensique, chiffrement renforcé, procédures juridiques et actions correctives (selon dépôts SEC).	https://www.cybersecuritydive.com/news/first-american-44k-breached-cyberattack/717377/
Mai-Dec 2023	Progress MOVEit	~2 600 organisations et ~85–90 millions d'individus touchés	Exploitation d'une vulnérabilité zero-day dans le logiciel MOVEit par le gang Cl0p (exploitation MFT → exfiltration). Correctifs de Progress, patching urgent, audits des	https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/

			transferts de fichiers, rotations de credentials, notification des victimes. Beaucoup d'organisations ont engagé analyses forensiques et mesures d'atténuation.	
Dec 2024 - Jan 2025	Cleo	Des dizaines d'organisations	Compromission de la solution MFT (chaîne d'attaque sur l'écosystème fournisseurs) ; publication/exfiltration par le groupe Cl0p. Investigations, notifications, mesures correctives chez Cleo et chez clients, recommandations de rotations de clés et segmentation.	https://www.opswat.com/blog/lessons-from-the-cleo-exploit-evidence-underscores-why-secure-mft-is-critical
Aout - Septembre 2025	Miljödata	Données RH sensibles pour employés	Ransomware / accès non autorisé au fournisseur HR (compromission fournisseur SaaS/tiers). Forensic et containment, notification aux parties affectées, renforcement des contrôles fournisseurs, révision des SLA de sécurité.	https://www.securityweek.com/volvo-group-employee-data-stolen-in-ransomware-attack/

Pour éviter ce genre de problèmes il existe plusieurs méthodes :
- Mettre à jour régulièrement les logiciels
- Utiliser des mots de passe forts et la double authentification
- Former le personnel contre le phishing
- Chiffrer et sauvegarder les données importantes (hashage)
- Surveiller les accès et contrôle la sécurité des fournisseurs

Conclusion

Ce TP m'a montré l'importance du hachage pour garantir l'intégrité des données. Un simple changement dans un fichier modifie totalement la valeur obtenue, ce qui en fait un moyen fiable pour détecter toute altération et vérifier l'authenticité des fichiers ou la sécurité des mots de passe.